

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Richmond Division

IN THE MATTER OF THE)
SEARCH OF INFORMATION ASSOCIATED) No. 3:22-sw- 128
WITH APPLE ID mesurontaylor@yahoo.com)
DS ID #1285532453)
THAT IS STORED AT PREMISES)
CONTROLLED BY APPLE, INC.)

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Tiffani L. Corley, being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I am a law enforcement officer within the meaning of Title 18, United States Code, § 2510(7), that is an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Title 18, United States Code, § 2516. I am presently employed as a Special Agent (“SA”) for the United States Drug Enforcement Administration (“DEA”). I have been employed full-time by the DEA since March 2005 and I am currently assigned to the Richmond District Office (“RDO”).

2. Prior to becoming an agent, I completed the DEA Basic Agent Training course in Quantico, Virginia, a seventeen-week intensive drug law enforcement-training program. DEA training focuses on, among other things: confidential informant (CI) management, interviews of suspects and defendants, report writing, physical and electronic surveillance, tactics, the preparation of wiretap affidavits and search warrants, and drug identification. After graduation, I successfully completed a sixteen-week field-training program at my first office of assignment. During my time as a Special Agent, I have participated in investigations involving the unlawful importation, exportation, manufacture, possession with intent to distribute and distribution of

narcotics, the laundering of narcotics proceeds, monetary instruments derived from narcotics activities, and conspiracies associated with narcotics offenses. I have participated in numerous narcotics investigations with more experienced SAs and Task Force Officers (“TFOs”) within DEA.

3. Through my training, experience, and interaction with other more experienced SAs, TFOs, and other narcotics investigators, I have become familiar with the methods employed by narcotics trafficking organizations to smuggle, safeguard, and distribute narcotics, and to collect and launder narcotics related proceeds. These methods include (but not limited to) the use of debit calling cards, public wifi hotspots, wireless communications technology (such as smartphone apps, voice over ip phones, and cellular telephones), counter surveillance, elaborately planned smuggling schemes tied to legitimate businesses, false or fictitious identities and coded communications in an attempt to avoid detection by law enforcement and circumvent narcotics investigations.

4. I have been involved in the preparation and service of California state and federal search warrants at numerous locations throughout the United States of America. At many of the locations, I have seized controlled substances including (but not limited to) cocaine, methamphetamine, MDMA, heroin, and marijuana. I have also seized many items of non-drug evidence, which include vehicles used to facilitate drug trafficking, narcotics proceeds, drug pay and owe sheets, telephone directories and toll records. I have interviewed many of the suspects at these locations, and I have learned of the methods and operations of the drug trafficking organizations.

5. In addition, I am familiar with narcotic traffickers’ methods of operation including the distribution, storage, and transportation of narcotics, the collection of money that

represent the proceeds of narcotics trafficking, and money laundering. I am aware narcotics traffickers often communicate with their drug trafficking associates through the use of many communications devices such as; home telephones, cell phones, and social media applications. I am aware drug traffickers will often change cellular telephones and account screen names to avoid detection by law enforcement. It has been my experience that narcotics traffickers will also use residential telephones, cellular telephones, and social media web sites that are not subscribed to their own names or addresses; as well as change these accounts frequently. They do this in order to avoid detection by law enforcement. It has been my experience that narcotics traffickers will also use registered vehicles, utilities, cellular telephones, and social media web sites that are not subscribed to their own names or addresses. They do this in order to avoid detection by law enforcement.

6. I have interviewed numerous criminals regarding the transportation and sales of narcotics. During many of these investigations, the criminals have admitted to their utilization of telephones, social media web sites, the utilization of stash locations, and methods of distribution. I know from my training and experience in the field of narcotics that subjects involved in the crimes of possession for sales and transportation of controlled substances will often utilize telephones and social web pages to arrange their crimes or coordinate with co-conspirators.

7. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

8. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter "Apple") to

disclose to the government records and other information, including the contents of communications, associated with the Apple ID mesurontaylor@yahoo.com and DS ID 1285532453 that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, CA. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

9. For the reasons stated below, there is probable cause to believe that the information described in Attachment A contains evidence, fruits and instrumentalities of violations of the following federal statutes: (1) Title 21, U.S.C. § 846 (conspiracy to possess with the intent to distribute controlled substances); (2) Title 21, U.S.C. § 841(a)(1) (possession with the intent to distribute controlled substances); and Title 21, U.S.C. § 843(b) (use of a communication facility to distribute controlled substances).

10. The statements in this affidavit are based in part on information provided by DEA Special Agents, other law enforcement officers, and on my experience and background as a Special Agent. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause for the requested warrant.

STATUTORY AUTHORITY

1. 21 U.S.C. § 846: prohibits a person from conspiring to knowingly manufacture, distribute, dispense, or possess with the intent to distribute a controlled substance.

2. 21 U.S.C. § 841(a)(1): prohibits a person from knowingly manufacturing, distributing, dispensing, or possessing with the intent to distribute a controlled substance

3. 21 U.S.C. § 843(b): prohibits a person from knowingly or intentionally using any communication facility in committing or causing or facilitating the commission of any act, or acts, constituting a felony under 21 U.S.C. § 841.

DEFINITIONS

1. The term “computer,” as defined in 18 U.S.C. §1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

2. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

3. “Internet Service Providers” (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

4. “Internet Protocol address” (IP address), as used herein, is a code made up of numbers separated by dots that identifies a particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the

ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

5. "Domain names" are common, easy to remember names associated with an IP address. For example, a domain name of "www.usdoj.gov" refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period.

6. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

INFORMATION REGARDING APPLE DEVICES AND iCloud¹

1. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

2. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage.

¹ The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at <http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf>; "Create and start using an Apple ID," available at <https://support.apple.com/en-us/HT203993>; "iCloud," available at <http://www.apple.com/icloud/>; "iCloud: iCloud storage and backup overview," available at <https://support.apple.com/kb/PH12519>; and "iOS Security," available at http://images.apple.com/privacy/docs/iOS_Security_Guide.pdf.

3. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

4. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

5. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

6. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs enables iCloud to be used to synchronize webpages opened in the Safari web browsers on all of the user’s Apple devices. iWorks Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

7. Game Center, Apple’s social gaming network, allows users of Apple devices to play and share games with each other.

8. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices.

9. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System (“GPS”) networks, and Bluetooth, to determine a user’s approximate location.

10. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

11. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services, which are accessible from both Apple devices and laptop and desktop computers. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

12. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be

associated with an Apple ID by the user.

13. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

14. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

15. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is

linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address (“MAC address”), the unique device identifier (“UDID”), and the serial number. In addition, information about a user’s computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user’s web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

16. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user’s photos and videos, iMessages, Short Message Service (“SMS”) and Multimedia Messaging Service (“MMS”) messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user’s instant messages on iCloud.

DETAILS OF INVESTIGATION

17. DEA Richmond Office has been conducting an ongoing narcotics investigation involving Mesuron TAYLOR and others both known and unknown to law enforcement. A review of TAYLOR's criminal history reveals (1) a 2004 federal conviction in the Eastern District of Virginia for possession of a firearm by a convicted felon, in which he was sentenced to 36 months imprisonment; (2) a 2005 felony possess, transport firearms by a convicted felon conviction in the Henrico County Circuit Court, in which he was sentenced to two years imprisonment; and (3) a 2016 conviction for transport/sell controlled substances in the Superior Court of California, Los Angeles County. As a result, prior to June 1, 2022, TAYLOR had previously been convicted of a crime punishable by imprisonment exceeding one year and knew he had previously been convicted of a crime punishable by imprisonment for a term exceeding one year.

18. In late August and early September 2020, the Augusta County Sheriff's Department conducted a controlled purchase operation against TAYLOR using CS#1.² As part of the operation, CS#1 contacted TAYLOR on the (310) 694-7122 and ordered approximately two pounds of methamphetamine. As part of the discussions, TAYLOR told CS#1 he would have another individual transport the methamphetamine to CS#1 in Augusta County within several days.

19. On September 3, 2020, based on information from CS#1, the Virginia State Police conducted a traffic stop on a vehicle driven by CS #2 in Augusta County, Virginia. During the course of the traffic stop, law enforcement officers recovered approximately two pounds of

² Subsequent to the controlled purchase, CS #1 self-reported to your affiant that leading up to this September 2020 transaction with TAYLOR, he/she had made several unauthorized purchases of methamphetamine from TAYLOR without approval from law enforcement.

methamphetamine from the vehicle.

20. On September 4, 2020, your affiant and DEA Task Force Officer (TFO) Adams Clarke interviewed CS#1 about TAYLOR's methamphetamine distribution. During this debrief, CS#1 positively identified a photograph of TAYLOR and provided the phone number (310) 694-7122 as TAYLOR's cellular telephone, the CS#1 also stated that they would rarely communicate other than using Facetime. CS#1 stated he/she contacted TAYLOR in the September 2020 on both the (310) 694-7122 and through social media applications to include Facebook messenger. Later in the debrief, in the presence of your affiant, CS#1 contacted TAYLOR on the (310) 694-7122 and TAYLOR answered. Your affiant heard a voice she identified as TAYLORS from previous recorded calls. During this monitored call, feigning ignorance of the two-pound methamphetamine seizure, CS#1 inquired about the expected arrival date of the methamphetamine she had previously ordered from TAYLOR. In response, TAYLOR stated he would follow up on the delay regarding the delivery of the methamphetamine.

21. Several days after the debrief, CS#1 provided your affiant with another video recorded call he/she made to TAYLOR to discuss the shipment of methamphetamine, all calls recorded from CS#1 were Facetime audio or video calls. Your affiant watched the video provided by CS#1 and confirmed by both video and audio that the subject was in fact TAYLOR. In the video recording of the call, CS#1 and TAYLOR once again discussed the methamphetamine purchase and CS#1 inquires as to when it will arrive. The voice of TAYLOR was identified as the same voice during the call made in the presence of your affiant.

22. On September 7, 2020, your affiant and DEA personnel interviewed CS#2. In this debrief, CS#2 stated in early September 2020 he/she received calls from TAYLOR on the (310) 694-7122 about delivering narcotics to a third party in the Central Virginia area. CS#2

stated he/she was provided an address by TAYLOR to deliver methamphetamine in Augusta County. Moreover, CS#2 stated he/she was instructed by TAYLOR to contact Whaki FOX, aka "Fee" about the narcotics delivery. CS#2 stated he/she contacted FOX by cellular phone and spoke about meeting to acquire narcotics. CS#2 stated after he/she met with FOX in Richmond, Virginia, he/she acquired methamphetamine to deliver to the third party in Augusta County. Agents also reviewed text messages from Fox to CS#2, which confirmed FOX met with CS#2 on the same date methamphetamine was transferred. After the narcotics were acquired from FOX, CS#2 stated she traveled to Augusta County and was stopped and arrested by Virginia State Police with approximately two pounds of methamphetamine in his/her possession.

23. Based on this CS information, your affiant investigated the (310) 694-7122 through a law enforcement database and learned it has been and is currently assigned to AT&T Mobility under the subscriber name of Mesuron TAYLOR. Your affiant also received a Pen Register for the mesurontaylor@yahoo.com Apple ID in March 2022. The return from Apple confirmed there were Facetime and iMessages to and from the mesurontaylor@yahoo.com Apple ID to many co-conspirators using his iPhone utilizing his AT&T account subscribed to his name.

24. In late September 2020, CS#2 informed your affiant that TAYLOR was flying into Richmond, Virginia. Your affiant contacted law enforcement at the Richmond International Airport and inquired about TAYLOR'S flight and arrival information. Your affiant was informed by law enforcement that TAYLOR was on DELTA flight 1325 which arrived in Richmond, Virginia, at 1931 hours on September 29, 2020. Your affiant was provided a picture of TAYLOR as he arrived into the airport. In that picture, TAYLOR could clearly be seen holding and using two cellular phones as he walked towards the rental car areas of the airport.

25. On October 1, 2020, your affiant and TFO Clarke observed an image of TAYLOR on an airplane, presumably a return flight from Richmond Virginia back to Los Angeles California. During TAYLOR'S time in Richmond, Virginia, your affiant and TFO Clarke were unable to track him to further identify his narcotics transactions in the Richmond metropolitan area.

26. On October 7, 2020, the Honorable Judge Roderick C. Young, United States District Judge, signed a geo-location search warrant to track the GPS location of the (310) 694-7122. The court order expired on November 6, 2020. During the month of October 2020, your affiant and TFO Clarke monitored the real time location of TAYLOR on TARGET TELEPHONE NUMBER. TAYLOR was tracked throughout Los Angeles, California, as well as traveling via plane from Los Angeles through Atlanta, Georgia, with a final destination in Richmond, Virginia. During TAYLOR'S time in Richmond, Virginia, your affiant and TFO Clarke attempted to locate where TAYLOR was staying in the greater Richmond area but were unable to pinpoint his exact location within numerous large buildings.

27. On October 28, 2020, a DEA CS (CS#3)³ was contacted by TAYLOR using Facebook Messenger and he advised he would like to meet with CS#3. TAYLOR also stated to CS#3 that he did not wish to talk over the phone but specifically wanted to meet in person. Your affiant and TFO Clarke met with CS#3 and then followed CS#3 to meet with TAYLOR. CS#3 met with TAYLOR is a 6th floor apartment in the Mezzo Lofts building at 17 W Broad Street in Richmond, Virginia. CS#3 stated TAYLOR advised he wanted to sell ounce quantities of heroin quickly while in Richmond for \$1700 per ounce so he did not have to travel back with heroin to

³ In April 2021, while a cooperating source, CS #3 was indicted and arrested for two offenses: (1) selling schedule I/II controlled substances with a firearm; and (2) possession with the intent to distribute schedule I/II controlled substance (offense date November 2020). In April 2022, CS#3 plead guilty to an amended charge of possession of schedule III controlled substance offense and was sentenced to a 12 month suspended sentence. The selling schedule I/II controlled substances with a firearm offense was nolle prossed.

Los Angeles. TAYLOR also advised CS#3 he would be traveling back to Los Angeles within several days.

28. On December 15, 2020, CS#3 met with TAYLOR and purchased approximately 56 grams of heroin. Prior to the meeting, CS#3 met with your affiant and ATF Task Force Officer Rodney Ward. CS#3 had previously negotiated a purchase of 2 ounces of heroin for \$4,000 from TAYLOR. CS#3 contacted TAYLOR using Facebook Messenger. TAYLOR answered the call and told CS#3 to come meet him downtown. The CS had previously met with TAYLOR in the downtown Richmond area.

29. CS#3 was given audio/video recording and transmission equipment and then left to meet with TAYLOR shortly after the call. Surveillance observed CS#3 arrive and park near the downtown meeting location. CS#3 entered the predetermined meeting location located in Richmond, Virginia. The conversation between CS#3 and TAYLOR was monitored by agents. Once CS#3 was inside the apartment with TAYLOR, CS#3 received the heroin and had a lengthy conversation regarding TAYLOR's drug trafficking activities. During the conversation TAYLOR asked CS#3 if he/she wanted "two grams or two ounces." The drug transaction between TAYLOR and CS#3 was captured on an audio/video recording.

30. CS#3 departed the apartment and immediately met with your affiant, ATF Task Force Officer Ward, and DEA Task Force Officer Christopher Clarke. CS#3 gave the heroin to your affiant, as witnessed by Task Force Officer Christopher Clarke. The heroin was subsequently sent to the DEA Mid-Atlantic Laboratory for testing. The DEA Laboratory returned results that the substance purchased from TAYLOR was heroin. CS#3 informed agents that the banging noise on the recording was TAYLOR breaking up a large "brick" of heroin to give it to CS#3. Based on my training and experience I know that heroin is transported in large

quantities in large, compressed bricks. Therefore, I believe that TAYLOR is receiving heroin in kilogram quantities.

31. In addition to the phone conversations between multiple CS and TAYLOR related to the several controlled purchases, law enforcement confirmed through AT&T that the wireless telephone number (310) 694-7122 is subscribed to Mesuron TAYLOR, with a listed address of 7515 S Denker Avenue, Los Angeles, California.

32. Your affiant has found the cellular handset utilizing phone account (310) 694-7122 to be an Apple iPhone through a subpoena to AT&T. Based on that information, DEA Richmond sent a subpoena to Apple, which identified TAYLOR's verified phone number to be (310) 694-7122 as having an Apple iCloud ID mesurontaylor@yahoo.com and DS ID 1285532453.

33. mesurontaylor@yahoo.com was listed as "Full iCloud" with the customer name as illmackabvich, which is the same user id for TAYLOR's Instagram page, and an address of 7515 S Denker Avenue, Los Angeles, California. All of these items were consistent with agent's knowledge of the investigation.

34. TFO Adams Clarke reviewed jail calls from TAYLOR. During this review TFO Clarke listened to a call between TAYLOR and his girlfriend. TAYLOR told her that he wished he could just delete his iCloud account, she agreed and said if she had TAYLOR's phones she would do it for TAYLOR. Based on my training and experience, from the above-mentioned conversation TAYLOR is aware that his iCloud account has further evidence of his narcotics trafficking.

35. I know from my training and narcotics experience persons engaged in the illegal distribution of narcotics often use cell phones to conduct their illegal business. Furthermore,

these individuals often store the names and telephone numbers of customers, co-conspirators, and sources of supply in the electronic memory of such devices. These individuals utilize the text messaging feature of the phone as well as download third party text message applications to communicate with customers and co-conspirators in an effort to avoid detection of Law Enforcement.

36. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

37. In addition to the communication features of cellular telephones, these devices also utilize a digital camera function to capture and store photographs and video within the device. It has been my experience that individuals engaged in the distribution of narcotics will often take pictures of narcotics, money and firearms for prestige and record keeping purposes.

38. I also know that cellular telephones are equipped with internal digital storage capabilities that often do not meet the needs of the user and cellular telephone users will often subscribe to a cloud type of offsite storage service such as iCloud to backup and store digital information from their cellular telephone in order to free up internal digital storage space on their cellular phone. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further

suspicion.

39. Based on the evidence in this investigation, your Affiant has probable cause to believe that stored messages, photos, contacts, and other information may be stored in the iCloud connected to TAYLOR's Apple ID mesurontaylor@yahoo.com. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity involving the investigation of the distribution of narcotics may be found in any of the files and records as described above summarizing Apple, and its services. This evidence may enable prosecutors to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

40. Other information connected to the Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal additional services used in furtherance of the crimes under investigation, including other apps and messaging services used by TAYLOR to distribute marijuana. For all of these reasons, Apple's servers are likely to contain stored electronic communications and information concerning its subscriber WEBB and his use of Apple's services and contain evidence of the distribution of narcotics crimes under investigation.

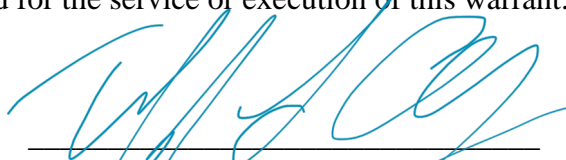
INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

41. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B,

government-authorized persons will review that information to locate the items described in Section II of Attachment B.


CONCLUSION

Based on the forgoing, I request that the Court issue the proposed search warrant. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.



Tiffani L. Corley
Special Agent, Drug Enforcement Administration

Sworn and subscribed before me
This ~~12th~~ day of July, 2022

_____/s/ 

Mark R. Colombell
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Apple ID mesurontaylor@yahoo.com and DS ID #**1285532453** (the “account”) that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to any request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A from the time period of **September 1, 2020 through June 1, 2022 (the date of TAYLOR's arrest)**:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber

Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), messaging logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);

g. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

h. All records pertaining to the types of service used; and

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I, including correspondence, records, documents, photographs, videos, applications, communications, and electronic messages that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252, and 2252A including, for each account or identifier listed on Attachment A, information pertaining to the following matters from the time period of **September 1, 2020 through June 1, 2022 (the date of TAYLOR's arrest)**:

- a. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);
- b. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;
- c. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);
- d. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and
- e. Evidence that may identify any co-conspirators or aiders and abettors for the above-listed crimes, including records that help reveal their whereabouts.